REAL-TIME CRYPTOGRAPHY FOR VITAL SIGNALS TRANSMISSION

Ding She Kion, Edmond Zahedi, Mohd. Alauddin Bin Mohd Ali

Electrical, Electronics and System Engineering Department, Faculty of Engineering
National University Malaysia

Abstract- **In this paper, an approach to design a real-time cryptography system for transferring vital signals is presented. The cryptography requirement is dictated by patient privacy. The system is divided into five main parts, namely symmetric encryption algorithms, key-exchange algorithm, hash function, communication protocol and display. The implemented algorithms are chosen based on parameters such as encryption speed, level of security and complexity. The key-exchange algorithm presented in this paper is based on the Diffie-Hellman key exchange protocol while SHA-1 hash function has been used as a component of authentication. A private message combined with Diffie-Hellman key is hashed to authenticate both parties. Finally, a communication protocol has been proposed for the system.**

Keywords: **telemetry, cryptography, authentication**

I. INTRODUCTION

With the rise of information technology, computers play an important role in everyday life, including handling of emergency cases. But transmission of medical data requires ensuring that this data is kept confidential, while the other requirement is authentication. Privacy ensures that transmitting messages that cannot be read or modified, while authentication allows each party to ascertain the identity of the other. Cryptography has done an excellent job in solving both problems.

The aim of this project is to develop a software running in the Microsoft Windows environment to encrypt and decrypt the biopotentials in real-time while providing authentication.

II. METHODS

A. System Architecture

The whole system can be subdivided into the following parts: signal acquisition, setting up a secure communication channel, transferring and displaying the signal. In this project, three different personal computers (PCs) are utilized to simulate different hardware devices in the system (fig. 1).

Bio-signals are usually acquired from a vital signs monitor/recorder e.g. an ECG monitor. In this project, we simulated the source of vital signals by a transmitting PC via a serial RS232 link. In fig. 1, the “Encryptor PC” and “Decryptor PC” take care of authentication as well as cryptography during transmission. The receiver PC (“Decryptor PC”) deciphers data before displaying it on the monitor. The connection between these PCs is a 100 Mbps Ethernet.

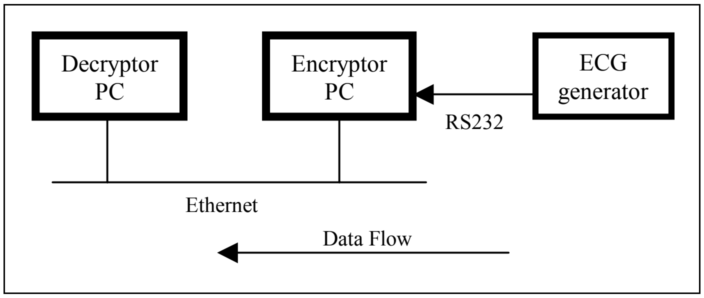

Fig. 1. System configuration based on three PC modules

LabView (National Instruments, Inc) and the concept of Virtual Instrument (VI) are used as a programming environment to acquire and display signals. The cryptography program itself is developed using C language.

B. Authentication & Cryptography

Among the various algorithms used in this work [1]-[3], only one is elaborated here: the Diffie-Hellman key-exchange algorithm [4] is employed for key exchange purposes. This protocol allows two parties that share common public-key and generator, agreeing on a new set of public-key and generator when they start communicating.

As a public-key in this protocol, a large prime (1024-bit) is used. This key is generated using Rabin-Miller prime generation [5].

The Secure Hash Algorithm revised version [6] (SHA-1) is used in this project as a message digest algorithm.

The overall operation of the authentication and cryptography sequences are shown in Fig. 2. For simplicity, Alice and Bob represent the two parties willing to communicate over an insecure channel.

0-7803-7211-5/01$10.00©2001 IEEE

Report Documentation Page

Report Date 25 Oct 2001	**Report Type** N/A	**Dates Covered (from... to)** -

Title and Subtitle Real-Time Cryptography for Vital Signals Transmission	**Contract Number**
	Grant Number
	Program Element Number
Author(s)	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) National University Malaysia Electrical, Electronics and System Engrg Dept Faculty of Engineering Malaysia	**Performing Organization Report Number**
Sponsoring/Monitoring Agency Name(s) and Address(es) US Army Research, Development & Standardization Group (UK) PSC 802 Box 15 FPO AE 09499-1500	**Sponsor/Monitor's Acronym(s)**
	Sponsor/Monitor's Report Number(s)

Distribution/Availability Statement
Approved for public release, distribution unlimited

Supplementary Notes
Papers from 23rd Annual International Conference of the IEEE Engineering in Medicine and Biology Society, October 25-28, 2001, held in Istanbul, Turkey. See also ADM001351 for entire conference on cd-rom.

Abstract

Subject Terms

Report Classification unclassified	**Classification of this page** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** UU

Number of Pages
4

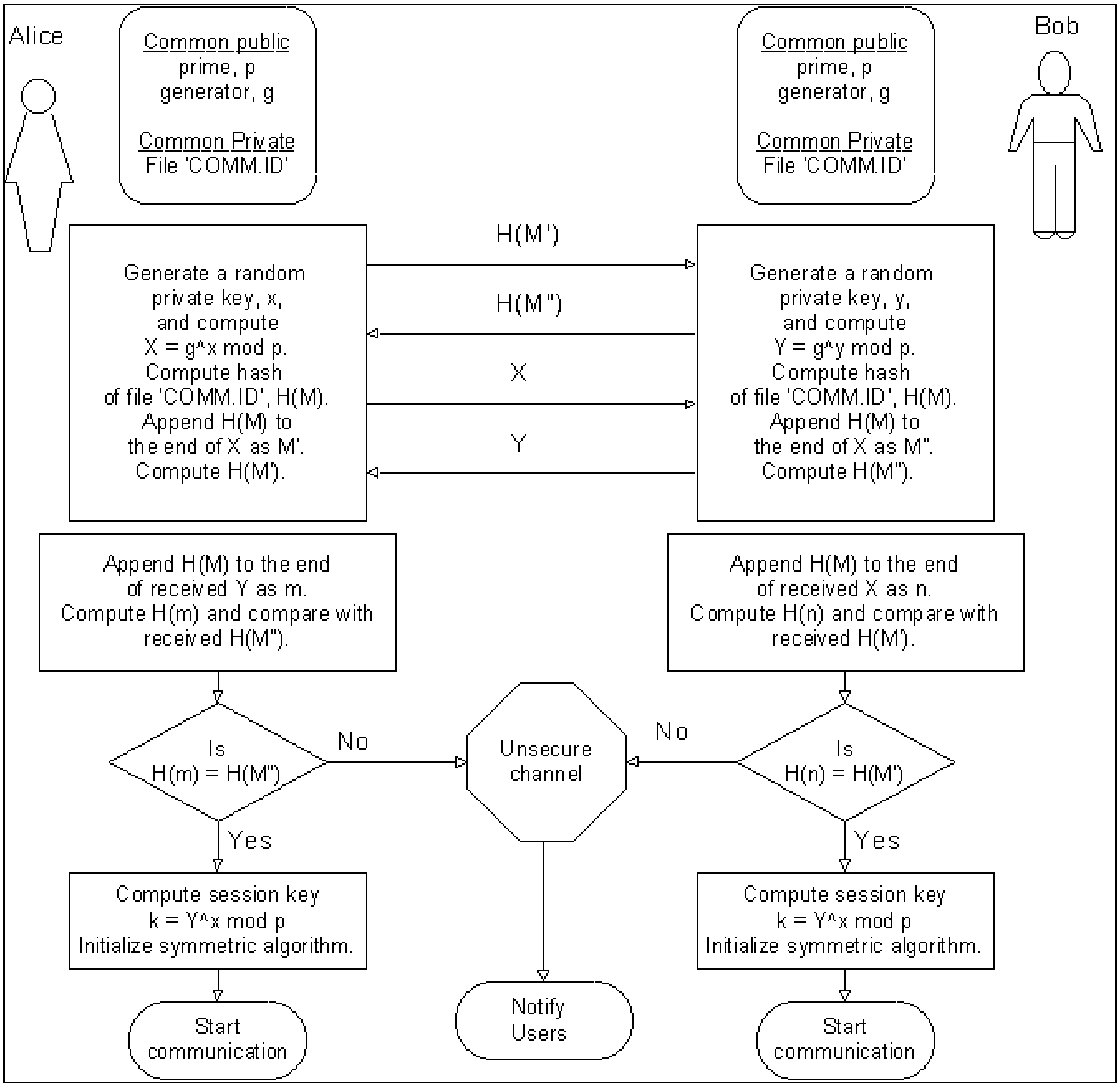
Alice
Common public
prime, p
generator, g
Common Private
File 'COMM.ID'
Bob
Common public
prime, p
generator, g
Common Private
File 'COMM.ID'
H(M')
H(M")
X
Y
Generate a random private key, x, and compute X = g^x mod p. Compute hash of file 'COMM.ID', H(M). Append H(M) to the end of X as M'. Compute H(M').
Generate a random private key, y, and compute Y = g^y mod p. Compute hash of file 'COMM.ID', H(M). Append H(M) to the end of X as M". Compute H(M").
Append H(M) to the end of received Y as m. Compute H(m) and compare with received H(M").
Append H(M) to the end of received X as n. Compute H(n) and compare with received H(M').
Is H(m) = H(M")
No
Unsecure channel
No
Is H(n) = H(M')
Yes
Yes
Compute session key k = Y^x mod p Initialize symmetric algorithm.
Compute session key k = Y^x mod p Initialize symmetric algorithm.
Start communication
Notify Users
Start communication

Fig. 2. Proposed procedure for authentication based on the Diffie-Hellman key-exchange protocol

After the authentication stage is terminated, normal Diffie-Hellman key-exchange algorithm is applied to get the session key. We can now use the session key to encrypt and decrypt messages between the two parties (Alice and Bob in fig. 2).

C. *Communication Protocol*

The Diffie-Hellman key-exchange program is installed in both encryptor and decryptor PCs and started automatically.

The two PCs will go through the Diffie-Hellman key-exchange algorithms as described above. Once the session key is successfully established, the program will be minimised and data encryption is systematically dine before transmission.

The second phase of the program activates a remote control software (NetOp, from DanWare Data A/S) in order to transmit and receive files. All these functions are achieved by using the ability of NetOp scripting and through NetOp OCX modules. The overall operation for data transfer and is shown in fig. 3.

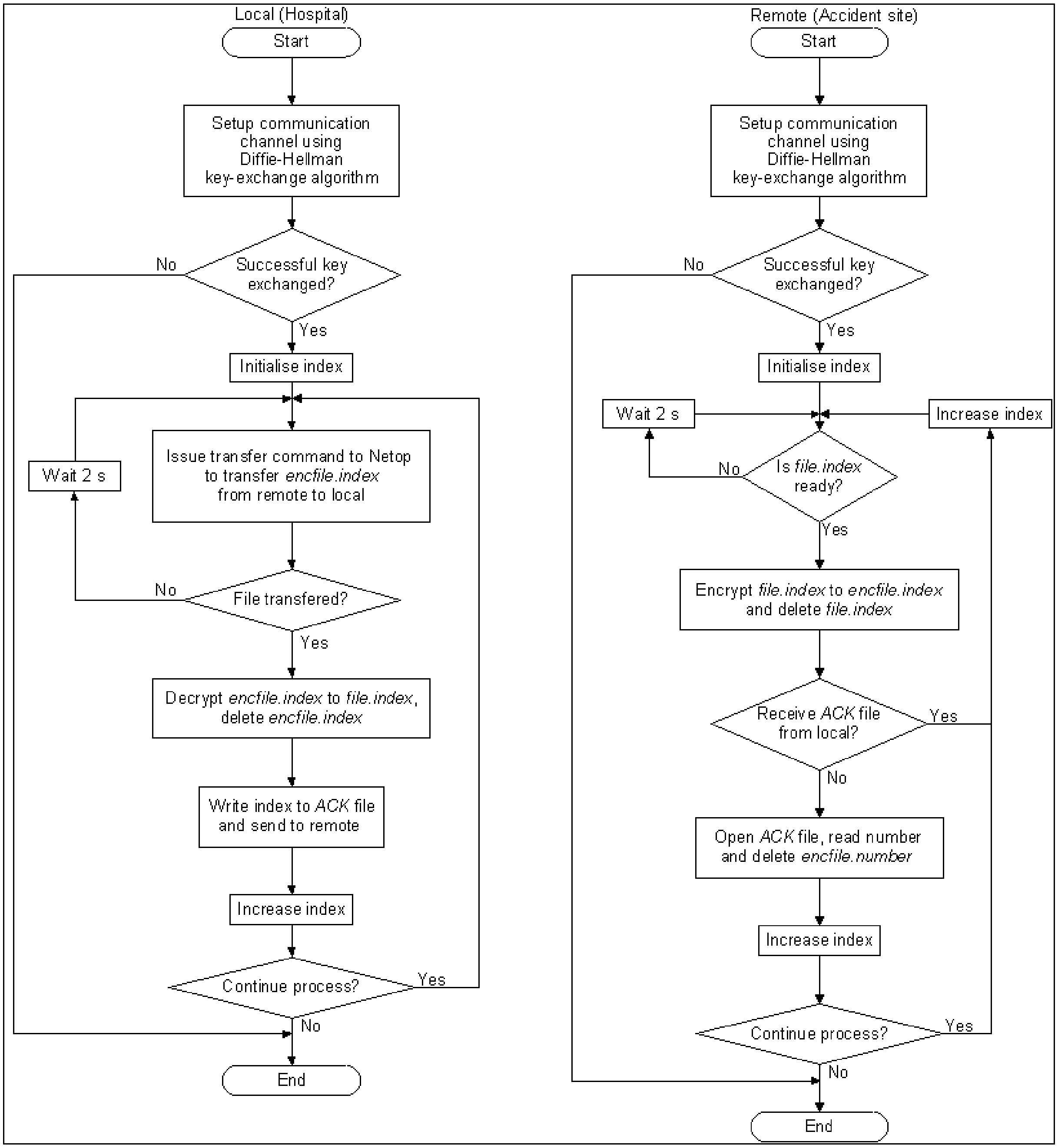
Local (Hospital)
Start
Setup communication channel using Diffie-Hellman key-exchange algorithm
Successful key exchanged?
No
Yes
Initialise index
Issue transfer command to Netop to transfer *encfile.index* from remote to local
Wait 2 s
File transfered?
No
Yes
Decrypt *encfile.index* to *file.index*, delete *encfile.index*
Write index to *ACK* file and send to remote
Increase index
Continue process?
Yes
No
End
Remote (Accident site)
Start
Setup communication channel using Diffie-Hellman key-exchange algorithm
Successful key exchanged?
No
Yes
Initialise index
Wait 2 s
Increase index
Is *file.index* ready?
No
Yes
Encrypt *file.index* to *encfile.index* and delete *file.index*
Receive *ACK* file from local?
Yes
No
Open *ACK* file, read number and delete *encfile.number*
Increase index
Continue process?
Yes
No
End

Fig. 3. Proposed communication protocol

D. *Data Display*

A local VI checks for the availability of a new data file and displays the ECG signal upon receipt of this new file.

E. *Hardware Platform*

For this system, 3 PCs are used in the laboratory environment. In the future, a single-board computer will replace the “Encryptor PC” which will be used at the accident area to communicate with the PC at the hospital.

CONCLUSION

This project is an early stage of development of a telemedicine project to be deployed in accident and emergency units. The system is intended for commercialisation once completed. However, some limitations have to be addressed: file transfer is used to send data. Due to this limitation, we are introducing some delay to the system. Work currently under progress is addressing these issues.

ACKNOWLEDGMENT

This work is sponsored by a grant from the Ministry of Science, Technology and the Environment of Malaysia under reference IRPA 04-02-02-0025.

REFERENCES

[1] B. Schneier, “Description of a New Variable-Length Key, 64-Bit Cipher (Blowfish),” *Fast Software Encryption, Cambridge Security Workshop Proceedings*, Springer-Verlag, 1994, pp. 191-204.

[2] X. Lai and J. Massey, “A Proposal for a New Block Encryption Standard,” *Advances in Cryptology – EUROCRYPT’90 Proceedings*, Springer-Verlag, 1991, pp.384-404.

[3] RFC 2144, "The CAST-128 Encryption Algorithm".

[4] W. Diffie and M.E. Hellman, “New Directions in Cryptography,” *IEEE Transactions on Information Theory*, Vol. IT-22, No. 6, November 1976, pp. 644-654.

[5] M. O. Rabin, “Probabilistic algorithm for primality testing,” *Journal Number Theory*, v. 12, n. 1, Feb 1980, pp. 128-138.

[6] *U.S. National Institute of Standards and Technology*, “Secure Hash Standard”, NIST FIPS PUB 180-1